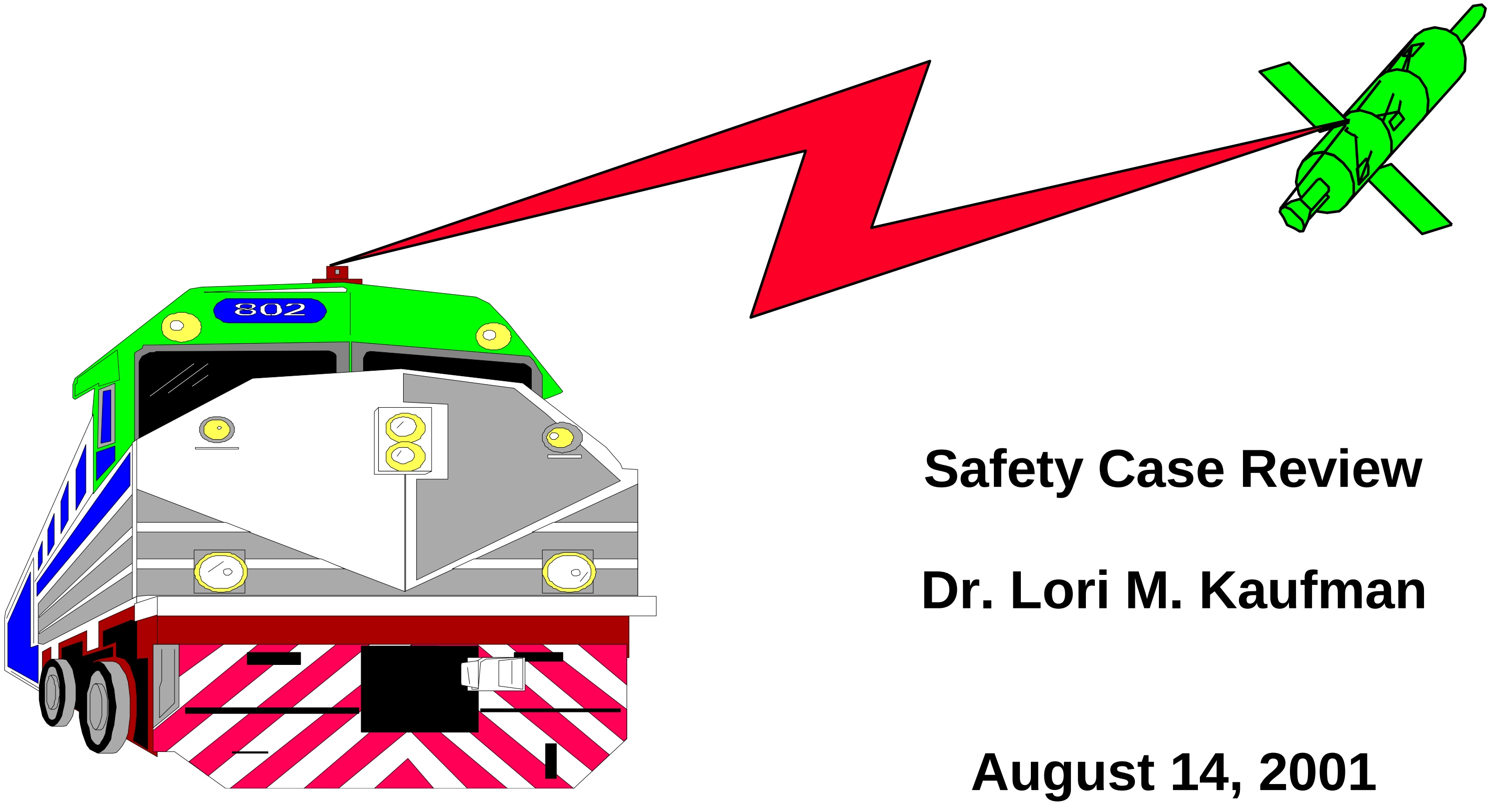
University of Virginia

School of Engineering
and Applied Science
Center for Safety-Critical Systems



Safety Case Review

Dr. Lori M. Kaufman

August 14, 2001

OUTLINE

- Preamble
- ASCAP Modeling
- Object Modeling
- Agent Modeling
- Blackboard Outcomes
- Traffic Management Algorithm (TMA)
- Train Speed Algorithm
- ASCAP In Action
- CBTM vs. DTC Mishap Results

PREAMBLE

SAFETY CASE SUBMITTAL TOPICS

- ASCAP Task Evolution
- ASCAP NPRM Draft Version #8 Compliance
- FRA "Adequacy and Calibration" Reviews
- Safety Case CRADA Submittal
- Proof-of-Concept Lessons Learned
- Work-IN-Progress (WIP)
- DTC/CBTM Safety Case Review "Slice"

ASCAP TASK EVOLUTION

- ASCAP evolved over the last three-years to support the Processor-Based Regulatory Rule

- Evolution has been from very simple disarrangement of interlocking processors to a system wide risk assessment methodology that allocates MTTHE compliance requirements that has followed the Standards Working Group Evolution

- FRA designated an “Adequacy and Calibration” Review Team in January 2001

- UVA committed to preparation of DTC/CBTM Safety Case to be submitted as a Draft Copy in June 2001 and final copy by September 2001

- The FRA Review Team concluded in July 2001 with ***Unanimous Approval*** that the ASCAP methodology approach meets the requirements for a competent method to support the Processor-based Rule

- Punch List enhancement items remain to be resolved

ASCAP NPRM DRAFT VERSION # 8 COMPLIANCE

- **ASCAP NPRM compliance provides a multi-faceted support**
  - **Risk assessment methodology based on train traffic exposure**
    - **Subject to a “high degree of confidence”**
  - **Allocation of MTTHE requirements for risk compliance**
  - **Repair rates and scheduled maintenance constraints**
  - **Integration of track plan, processor-based signaling and train control**
  - **Human-factors integrated with the physical track plan and rolling stock**
  - **Sequence of events, human-factors, track plan and rolling stock integration that leads to a mishap, incident or accident construction**
  - **Data mining to validate & verify human-factors, mechanical, communications and processor-based models**

FRA “ADEQUACY AND CALIBRATION” REVIEWS

Review Team concluded in July 2001, with <u>Unanimous Approval</u>, that the ASCAP methodology approach was acceptable to support the Processor-Based Rule Safety Assessment Requirements

- **The FRA Review Teams considered the following topics:**
  - **Traffic Management Algorithm (TMA)**
  - **CBTM functional operation**
  - **Human-factors framework and modeling**
  - **DTC/CBTM ASCAP data base(s)**
  - **Sensitivity analysis and severity model**
  - **MTTHE compliance**
  - **Safety Case structure and content**

SAFETY CASE CRADA SUBMITTAL

- **September 2001 Safety Case submittal concludes the ASCAP Proof-of-Methodology**
  - **Specified by the Proposed TASK 9 of the Nuclear Regulatory Commission (NRC) Cooperative Research and Development Agreement (CRADA)**
- **FRA shall develop a “Punch List” of outstanding items to be resolved as a new ASCAP program to be defined**

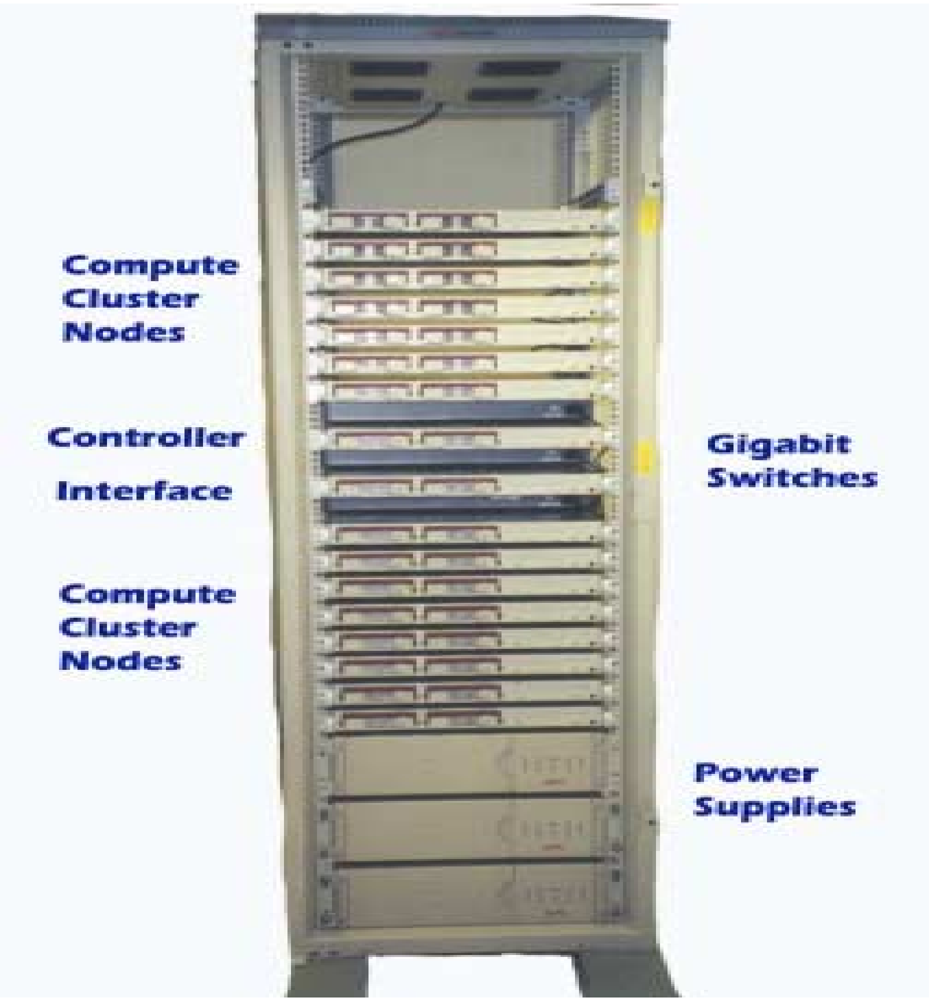
PROOF-OF-CONCEPT LESSONS LEARNED

- **ASCAP supports the processor-based language risk assessment and MTTHE compliance requirements**
- **Large knowledge gap between ASCAP builders ant the user community**
- **Need to move from an ASCAP “adequacy & calibration” process to a rigorous formal methods validation and process**
- **ASCAP simulation engine must be developed as an application independent parallel processing simulation engine**
- **FRA data collection long term strategy must adopt an approach that is consistent with risk assessment methodology**

WORK-IN-PROGRESS (WIP)

- **Current ASCAP Work-in-Progress Programs**
  - **LMC/IDOT:**
    - **Safety design support**
    - **Risk assessment**
    - **MTTHE compliance**
  - **New York City Transit (NYCT):**
    - **Risk assessment**
    - **MTTHE compliance**
  - **Maglev “Pennsylvania Project”**
    - **Risk assessment**
    - **Real-time control system simulation**
    - **Parallel processor and predictive tool set**

PARALLEL PROCESSING PLATFORM



DTC/CBTM SAFETY CASE REVIEW “SLICE”

- Safety Case presents a DTC/CBTM example
  - Illustrates the ASCAP methodology
  - Illustrates the Safety Case approach
- Safety Case submitted
  - Represents a demonstration of the methodology
  - Recommends the contents and substance of a Safety Case that would be submitted to the FRA
- DTC/CBTM Proof-of-Concept demonstrates that CBTM holds strong promise to meet the Designer Objectives and claims of improved safety-critical performance

SAFETY CASE

ASCAP MODELING

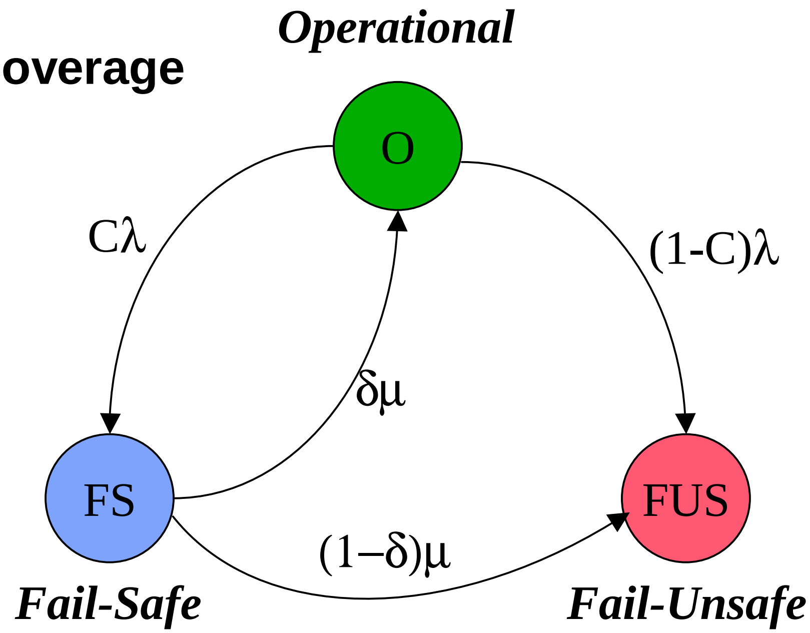
- Two model constructs
  - Object
    - Represent physical entities
      - Stationary
      - Mobile
    - Reactive
  - Agent
    - Represent human behavior
      - Dispatcher
      - Train Crew
      - Roadway Worker
    - Proactive

ASCAP MODELING

- **Model interactions determine train movement modalities**
  - **Movement modalities extracted from CSX operating rules**
    - **Represented as *Blackboard Outcomes***
      - **Function of agent(s) state**
      - **Function of object(s) state**
    - **Sequencing of *Blackboard Outcomes* generate mishap scenarios**

OBJECT MODELING

- **λ: failure rate**
- **μ: repair rate**
- ***C*: physical device coverage**
- **δ: repair coverage**



- **Generalized distributions can be used within model**

OBJECT MODELING

- **ASCAP Stationary Objects**
  - **DTC**
    - **Switch**
    - **Speed Zone Sign**
    - **Block Boundary Sign**
    - **Broken Rail**
  - **CBTM**
    - **Manual Monitored Switch**
    - **Manual Unmonitored Switch**
    - **Speed Zone Sign**
    - **Block Boundary Sign**
    - **Broken Rail**
    - **Onboard Sub-system**
    - **Base Stations**
    - **Zone Logic Controllers**
    - **FEP/CC & COS**

OBJECT MODELING

DTC/CBTM		CBTM	
OBJECT	NUMBER OF OBJECTS	OBJECT	NUMBER OF OBJECTS
SWITCH	63*	ON-BOARD SUB-SYSTEM	ALL TRAINS
SPEED ZONE SIGN	36	BASE STATIONS	8
BLOCK BOUNDARY SIGN	40	ZONE LOGIC CONTROLLERS	2
BROKEN RAIL	128	FEP/CC & COS	1

*For CBTM, 21 switches are monitored

OBJECT MODELING

DTC/CBTM					
OBJECT	FAILURE RATE (failures/hr)	COVERAGE	REPAIR RATE (repairs/hr)	REPAIR COVERAGE	M&II (days)
SWITCH	4 X 10^{-5}	0	0.125	0.99995	4
SPEED ZONE SIGN	1 X 10^{-6}	0	0.125	0.99995	4
BLOCK BOUNDARY SIGN	5 X 10^{-7}	0	0.125	0.99995	4
BROKEN RAIL	1 X 10^{-5}	0, 0.3, 0.6, 0.9	0.125	0.99995	4

OBJECT MODELING

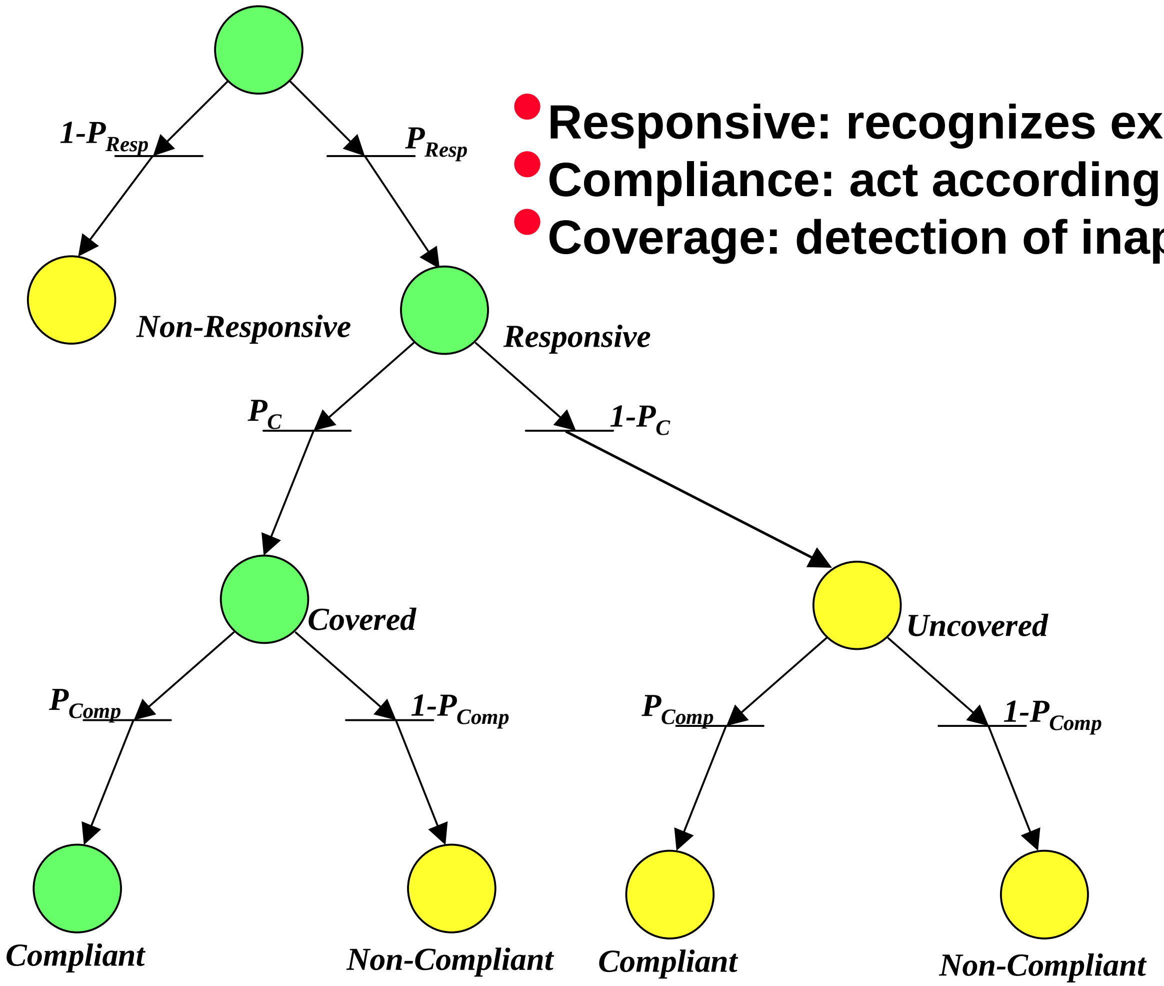
CBTM						
OBJECT	FAILURE RATE (failures/hr)	ADJUSTED FAILURE RATE (failures/hr)	COVERAGE	REPAIR RATE (repairs/hr)	REPAIR COVERAGE	M&II (days)
ONBOARD SUB-SYSTEM	1.6 X 10^{-4}	8.0 X 10^{-4}	0.7, 0.9, 0.95	0.125	0.99995	4
BASE STATION	2.1 X 10^{-4}	1.05 X 10^{-3}	0.7, 0.9, 0.95	0.125	0.99995	4
ZONE LOGIC CONTROLLER	2 X 10^{-5}	1.0 X 10^{-4}	0.7, 0.9, 0.95	0.125	0.99995	4
FEP/CC & COS	4 X 10^{-5}	2.0 X 10^{-4}	0.7, 0.9, 0.95	0.125	0.99995	4

- Failure rate must be adjusted to account for transient faults
  - 80 – 90% faults are transient
  - Manufacturer’s failure rates represent only permanent faults
  - Multiply manufacturer’s failure rates by 5 (80%)

OBJECT MODELING

- Mobile Objects
  - Unit trains
  - Intermodals
  - Merchandise
  - Locals

AGENT MODELING



- **Responsive: recognizes existence of stimuli**
- **Compliance: act according to stimuli**
- **Coverage: detection of inappropriate stimuli**

AGENT MODELING

- ASCAP Agents
  - DTC
    - Train Crew
    - Dispatcher
    - Roadway Worker
  - CBTM
    - Train Crew
    - Dispatcher
    - Roadway Worker

AGENT MODELING

AGENT	RECOGNITION HEP	HUMAN COVERAGE	COMPLIANCE HEP
DISPATCHER	1.96×10^{-4}	0.9	9×10^{-6}
TRAIN CREW	1.96×10^{-4}	0.999 – Agent Interaction 0.8 – Object Interaction	9×10^{-6}
ROADWAY WORKER	1.96×10^{-4}	0.999	9×10^{-6}

BLACKBOARD OUTCOMES

- Agent - To - Agent
  - Train Crew & Dispatcher
  - Train Crew and Roadway Worker (Employee In Charge)
- Agent - To - Object
  - Train Crew & Track Appliance
  - Train Crew & Track Feature

BLACKBOARD OUTCOMES

DTC Train Crew Action Resulting from Dispatcher/EIC Response

CREW BEHAVIOR	DISPATCHER BEHAVIOR				
	$P_{CovComp}$	P_{CovN-C}	$P_{UncovComp}$	$P_{UncovN-C}$	P_{N-R}
$P_{CovComp}$	Authority granted: train moves Authority denied: train does not move	Re-request authority Train movement stopped	Correct Authority Authority granted: train moves Authority denied: train does not move Incorrect Authority Re-request authority Train movement stopped	Recognize wrong authority Re-request authority Train movement stopped	Re-request authority Train movement stopped
P_{CovN-C}	Authority granted: train does not move Authority denied: train moves	Continue current movement	Correct Authority Authority granted: train stops Authority denied: train moves Incorrect Authority Continue current movement	Continue current movement	Continue current movement
$P_{UncovComp}$	Authority granted: train moves Authority denied: train does not move	Authority granted: train moves Authority denied: train does not move	Authority granted: train moves Authority denied: train does not move	Authority granted: train moves Authority denied: train does not move	Re-request authority Train movement stopped
$P_{UncovN-C}$	Authority granted: train does not move Authority denied: train moves	Authority granted: train does not move Authority denied: train moves	Authority granted: train does not move Authority denied: train moves	Authority granted: train does not move Authority denied: train moves	Continue current movement
P_{N-R}	Re-request authority Movement stopped	Re-request authority Movement stopped	Re-request authority Train movement stopped	Re-request authority Train movement stopped	Re-request authority Train movement stopped

BLACKBOARD OUTCOMES

DTC Train Crew Action Resulting from Dispatcher/EIC Response

CREW BEHAVIOR	DISPATCHER BEHAVIOR				
	$P_{CovComp}$	P_{CovN-C}	$P_{UncovComp}$	$P_{UncovN-C}$	P_{N-R}
$P_{CovComp}$	Authority granted: train moves Authority denied: train does not move	Re-request authority Train movement stopped	Correct Authority Authority granted: train moves Authority denied: train does not move Incorrect Authority Re-request authority Train movement stopped	Recognize wrong authority Re-request authority Train movement stopped	Re-request authority Train movement stopped

BLACKBOARD OUTCOMES

DTC Train Crew Action Resulting from Dispatcher/EIC Response

CREW BEHAVIOR	DISPATCHER BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_{CovN\text{-}C}$	Authority granted: train does not move Authority denied: train moves	Continue current movement	Correct Authority Authority granted: train stops Authority denied: train moves Incorrect Authority Continue current movement	Continue current movement	Continue current movement

BLACKBOARD OUTCOMES

DTC Train Crew Action Resulting from Dispatcher/EIC Response

CREW BEHAVIOR	DISPATCHER BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_{UncovComp}$	Authority granted: train moves Authority denied: train does not move	Authority granted: train moves Authority denied: train does not move	Authority granted: train moves Authority denied: train does not move	Authority granted: train moves Authority denied: train does not move	Re-request authority Train movement stopped

BLACKBOARD OUTCOMES

DTC Train Crew Action Resulting from Dispatcher/EIC Response

CREW BEHAVIOR	DISPATCHER BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_{UncovN\text{-}C}$	Authority granted: train does not move Authority denied: train moves	Authority granted: train does not move Authority denied: train moves	Authority granted: train does not move Authority denied: train moves	Authority granted: train does not move Authority denied: train moves	Continue current movement

BLACKBOARD OUTCOMES

DTC Train Crew Action Resulting from Dispatcher/EIC Response

CREW BEHAVIOR	DISPATCHER BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_{N\text{-}R}$	Re-request authority Movement stopped	Re-request authority Movement stopped	Re-request authority Train movement stopped	Re-request authority Train movement stopped	Re-request authority Train movement stopped

BLACKBOARD OUTCOMES

DTC Block Sign and Train Crew Agent Interaction

OBJECT STATE	TRAIN CREW BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_O(t)$	Request authority for next block Stop train	Do not request authority Continue train movement	Request authority for next block Stop train	Do not request authority Continue train movement	Do not request authority Continue train movement
$P_F(t)$	Request authority for next block Stop train	Do not request authority Continue train movement	Do not request authority Continue train movement	Do not request authority Continue train movement	Do not request authority Continue train movement

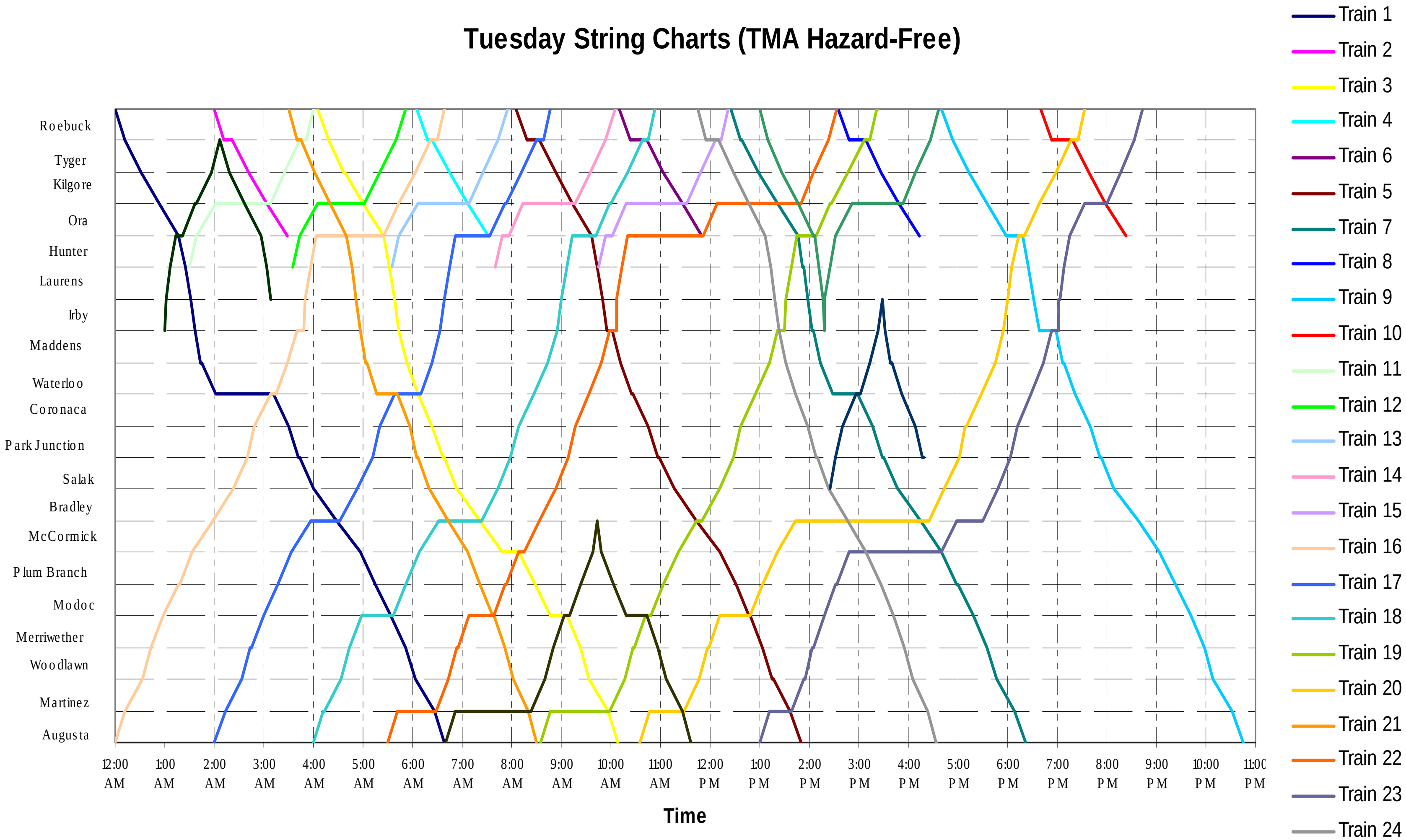
TRAFFIC MANAGEMENT ALGORITHM (TMA)

- TMA provides logical representation of CSX operating rules
  - CSX operating rules are assumed to be correct
  - CSX operating rules are assumed to specify all conditions for the system operation in a hazard-free and violation-free environment
    - All human behavior is compliant to the rules
    - All appliances are operational
- Schedule provided by CSX Transportation
- TMA is not an optimum line scheduler
  - Provides a set of feasible routes
  - Defines risk exposure

TRAFFIC MANAGEMENT ALGORITHM (TMA)

- TMA constraints/assumptions
  - Loaded unit trains can never occupy a siding
  - Yards and spurs serve as sources and sinks for the trains
  - Loaded trains have priority
  - Sidings are used solely to divert lower priority traffic from the main track
  - An empty siding always exist between two trains on the mainline
  - Once a train enters a siding, it is not allowed to re-enter the mainline if a clear route to the next empty siding does not exist
  - All train lengths can be accommodated by the sidings
  - Limit siding access to one train
  - Train movement is regulated on a per block basis
  - South bound train have priority
  - Use of pushers is not considered

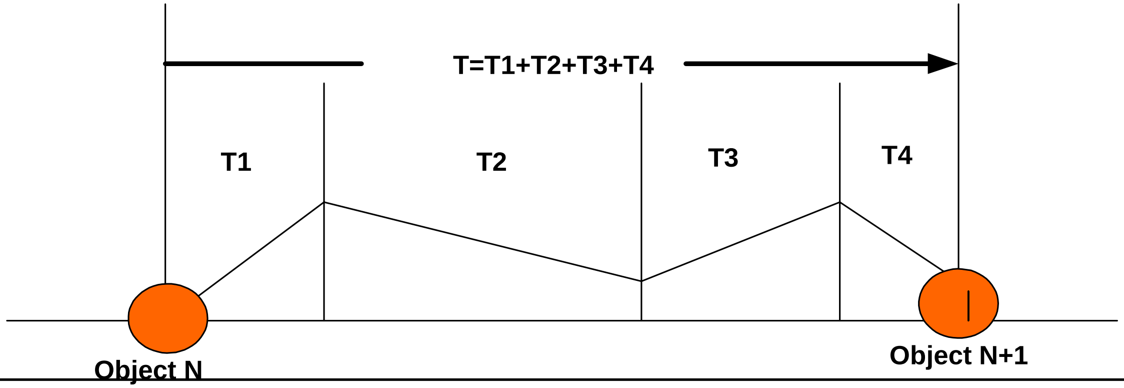
TRAFFIC MANAGEMENT ALGORITHM (TMA)



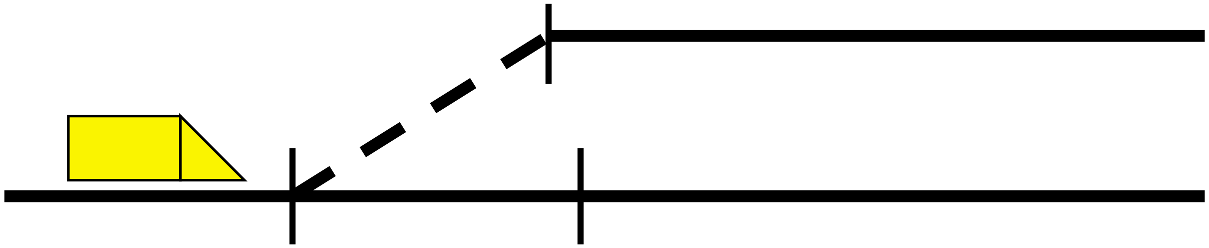
Tuesday String Charts (TMA Hazard-Free)

TRAIN SPEED ALGORITHM

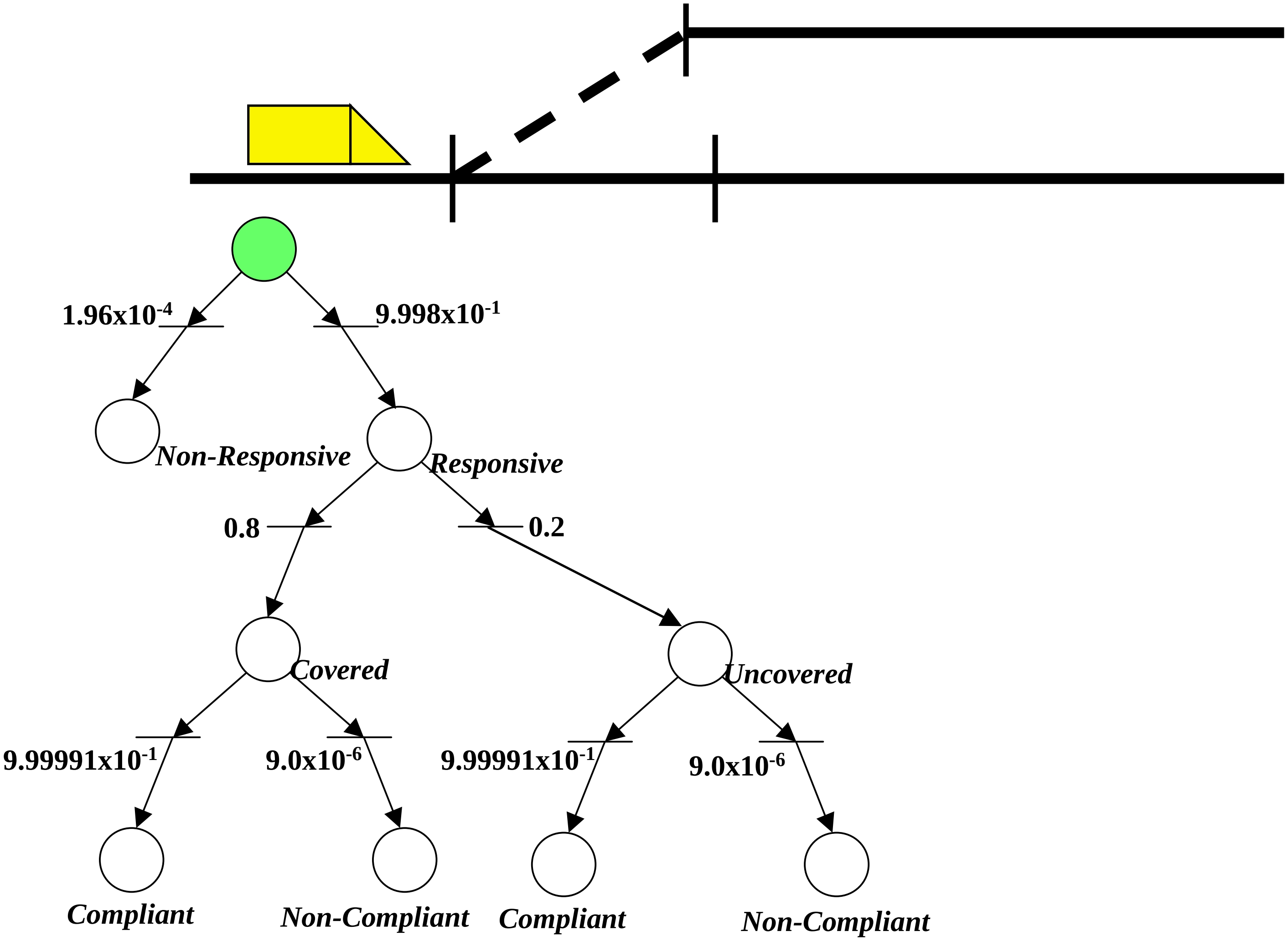
- Uses expert opinion and probabilistic look-ahead approach
- ASCAP “Gold Standard”
  - STEP 1: divide track plan between successive objects based on grade slope
  - STEP 2: use a normal distribution to approximate train speed and the standard deviation represents variations in speed as a function of the locomotive traction power and resistive and grade forces
  - STEP 3: select speed for each partition using a Monte Carlo selection where the partition speed and the standard deviation are generated probabilistically



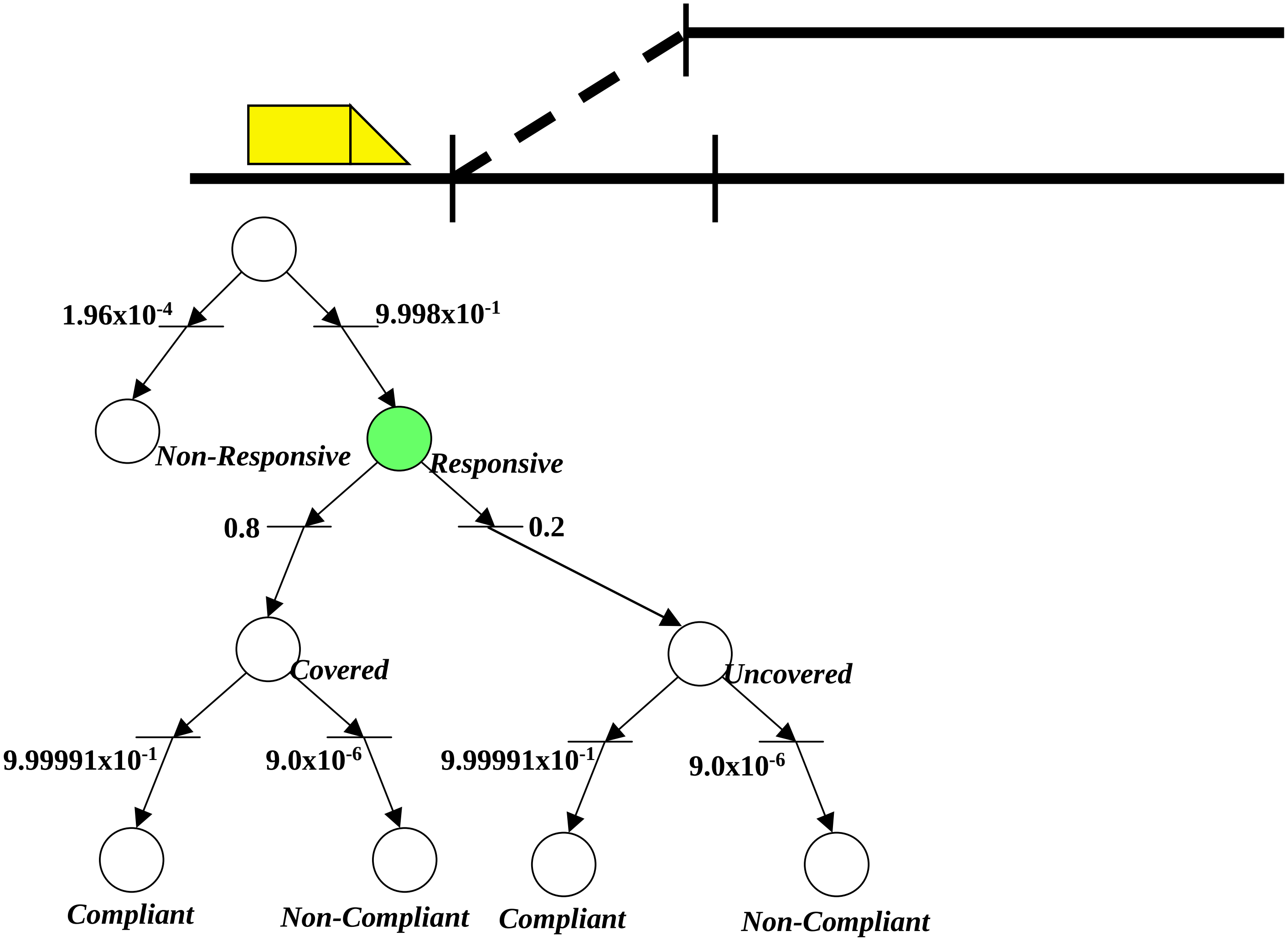
ASCAP IN ACTION



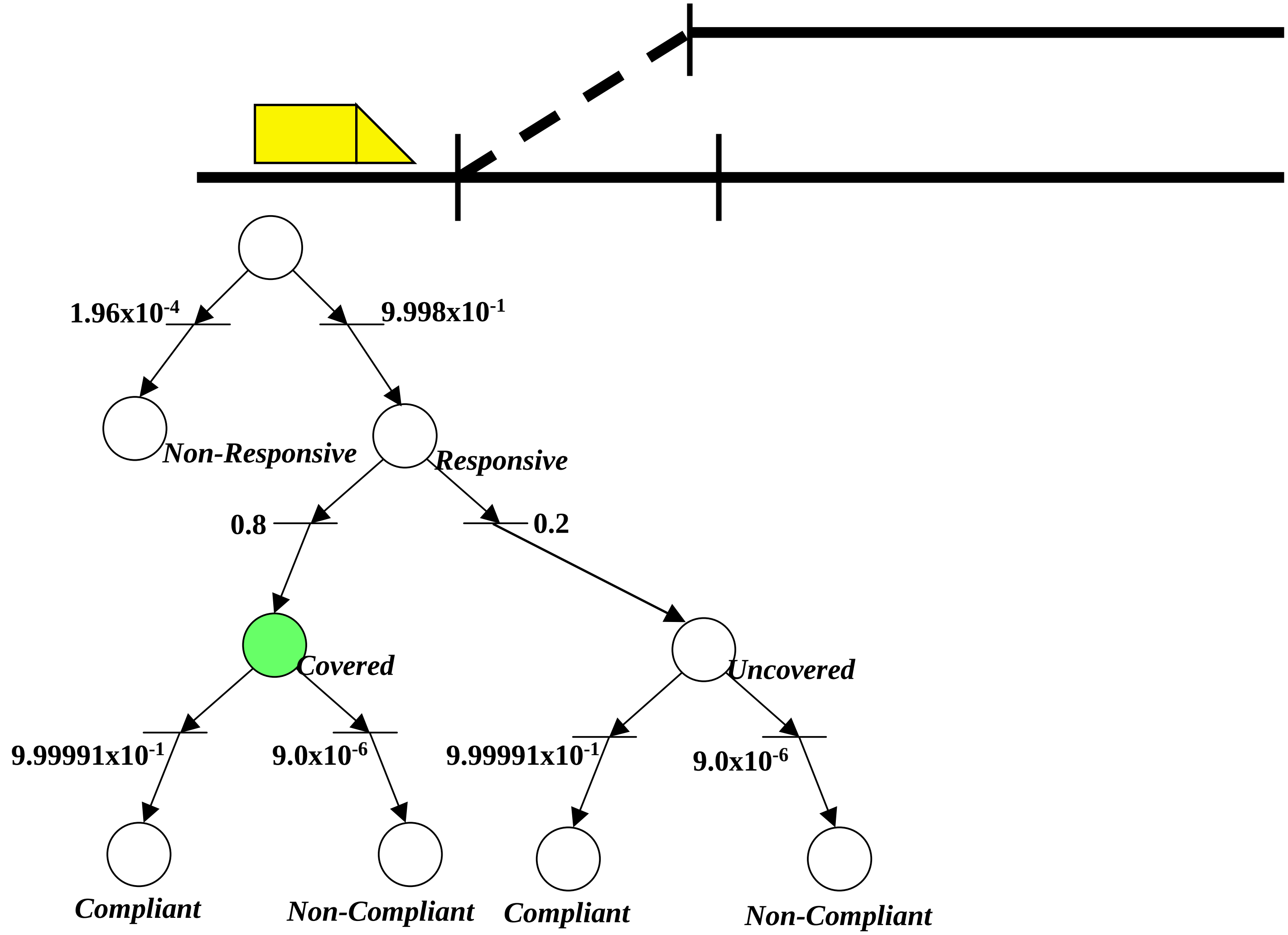
ASCAP IN ACTION



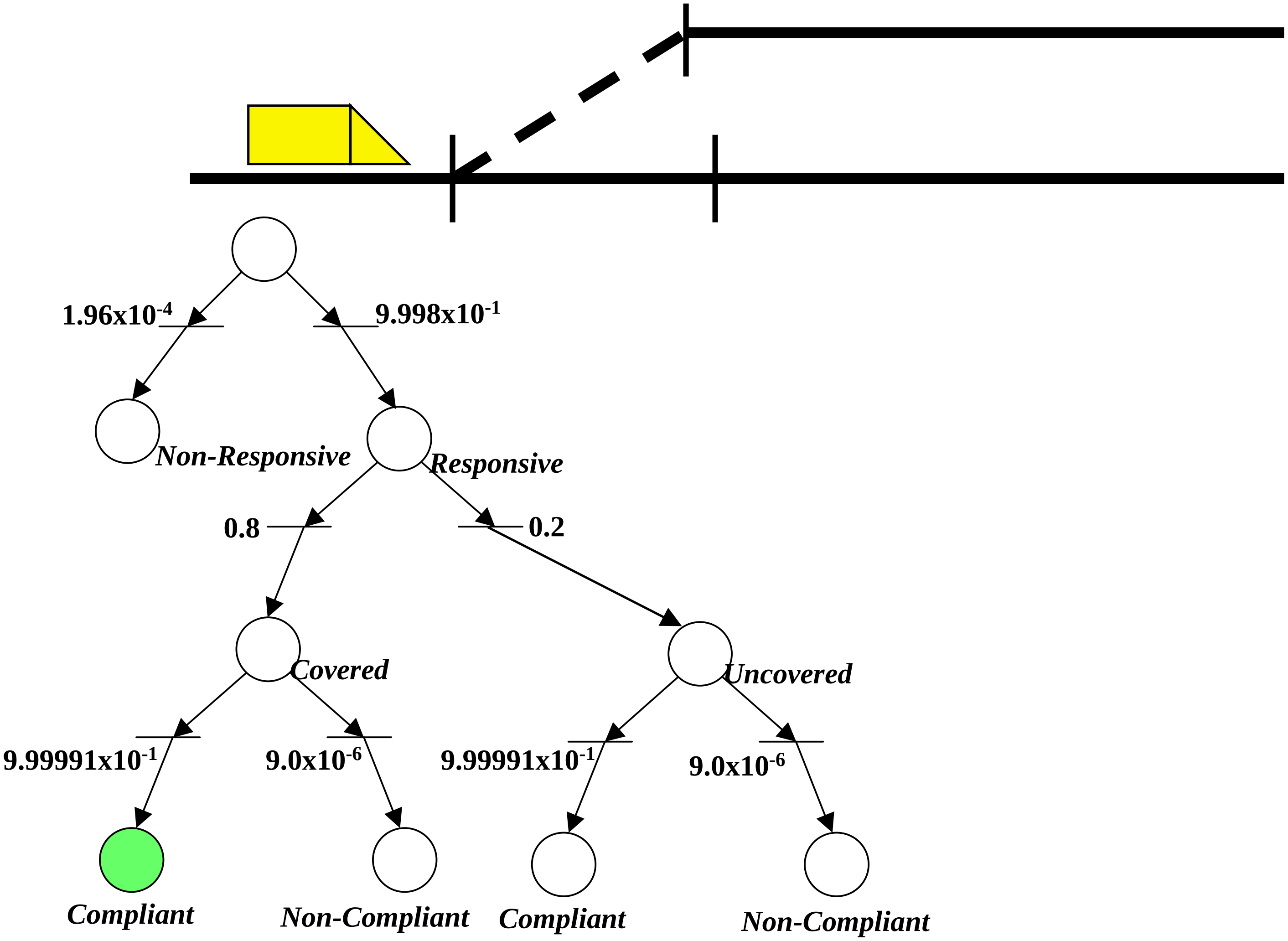
ASCAP IN ACTION



ASCAP IN ACTION



ASCAP IN ACTION



Non-Responsive

Responsive

Covered

Uncovered

Compliant

Non-Compliant

Compliant

Non-Compliant

$1.96x10^{-4}$

$9.998x10^{-1}$

0.8

0.2

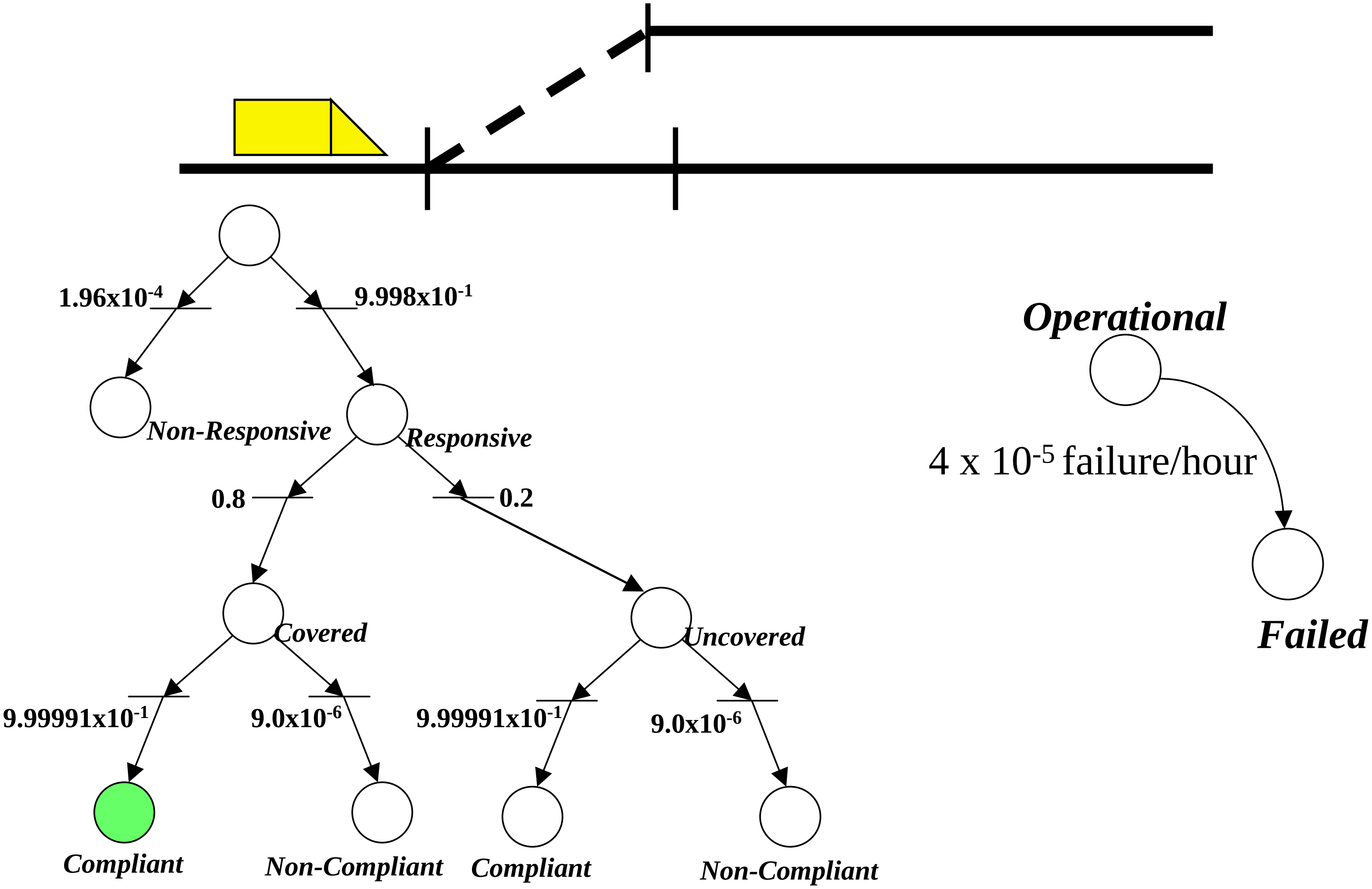
$9.99991x10^{-1}$

$9.0x10^{-6}$

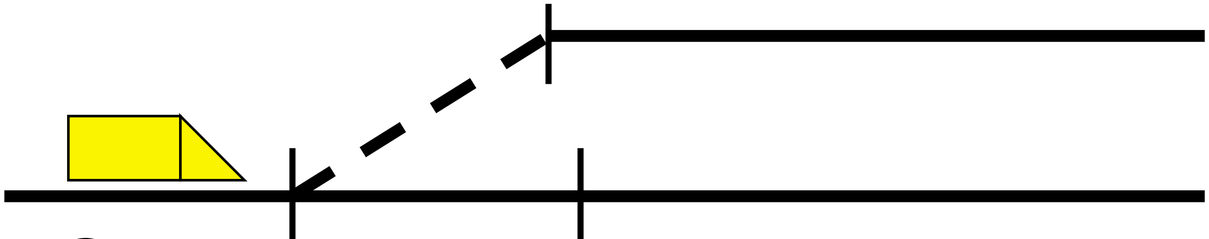
$9.99991x10^{-1}$

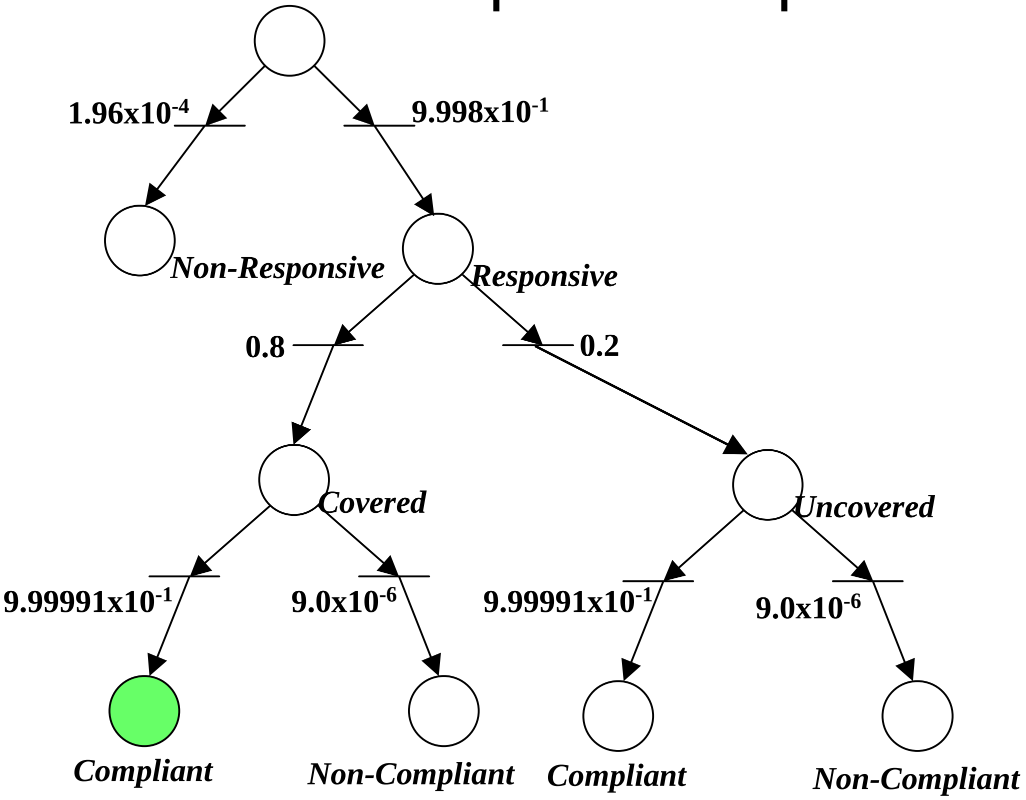
$9.0x10^{-6}$

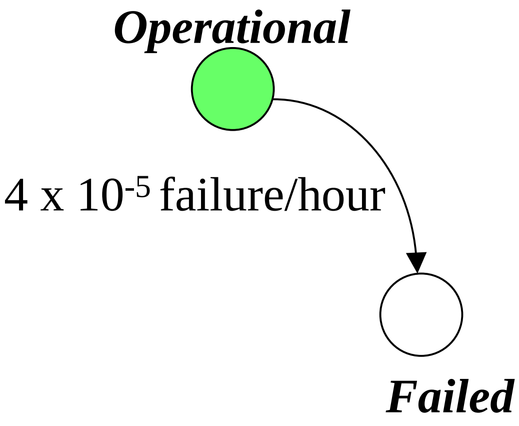
ASCAP IN ACTION



ASCAP IN ACTION



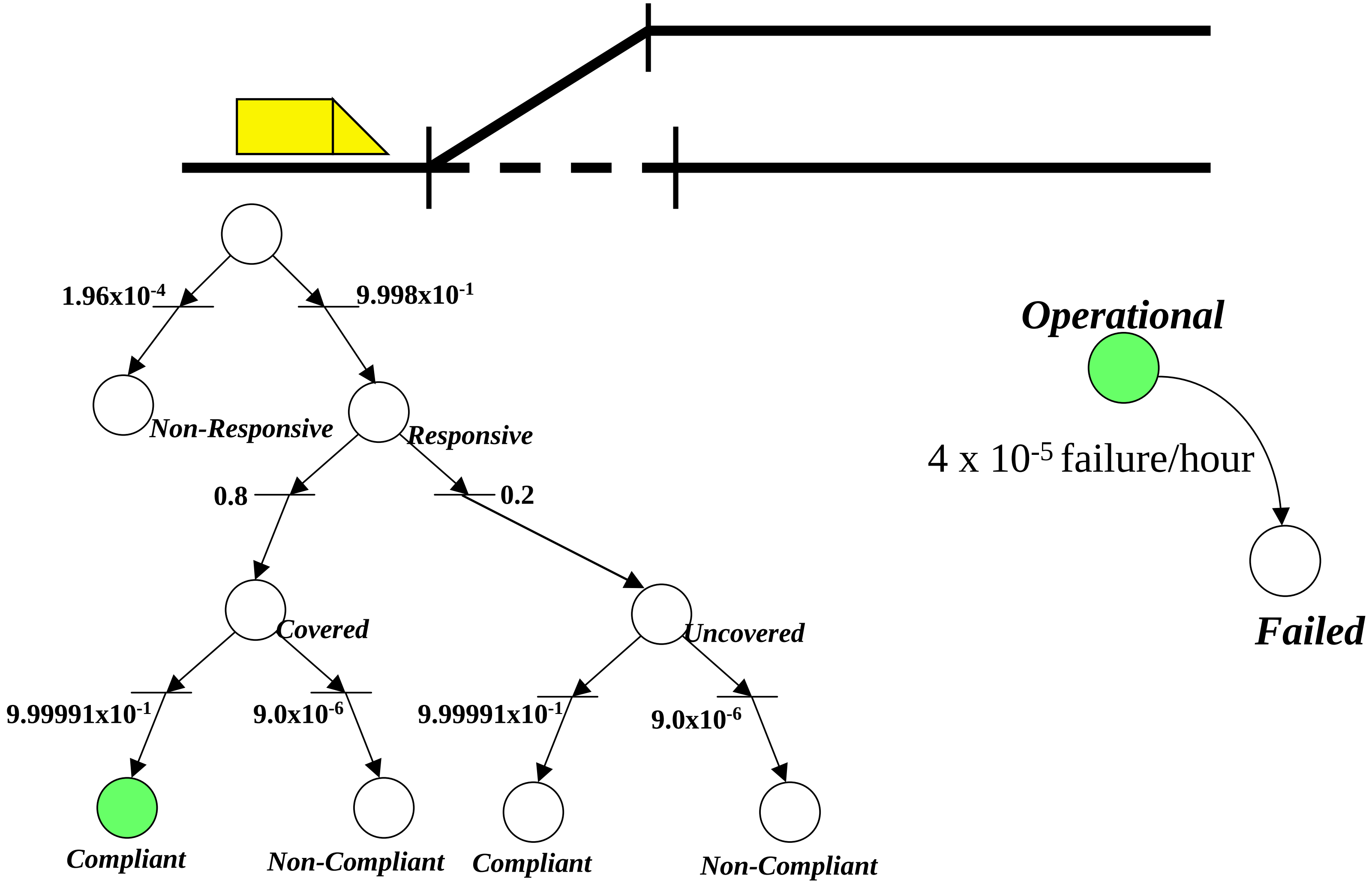




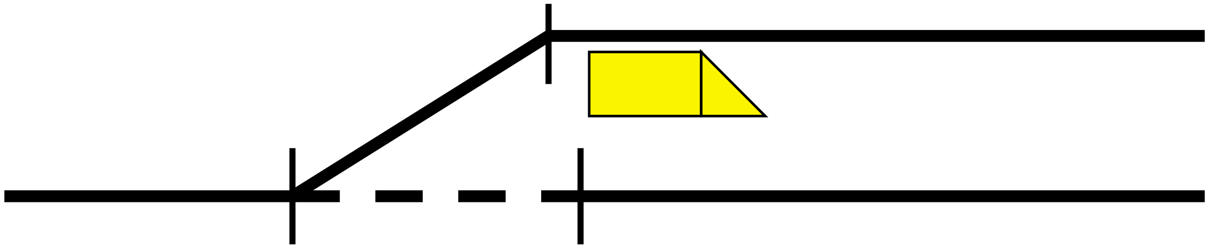
ASCAP IN ACTION

OBJECT STATE	TRAIN CREW BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_O(t)$ - Normal	Stop train Set reverse Continue to siding Clear switch point	Continue movement on main	Stop train Set reverse Continue to siding Clear switch point	Continue movement on main	Continue movement on main
$P_O(t)$ - Reverse	Stop train Keep reverse Continue to siding Clear switch point	If speed > 8 mph then MISHAP Else continue to siding & clear switch point	Stop train Keep reverse Continue to siding Clear switch point	If speed > 8 mph then MISHAP Else continue to siding & clear switch point	If speed > 8 mph then MISHAP Else continue to siding & clear switch point
$P_F(t)$ - Normal	Stop train Report failure Await repair Continue to siding Clear switch point	Continue movement on main	Stop train Believe switch set reverse Continue on main	Continue movement on main	Continue movement on main
$P_F(t)$ - Reverse	Stop train Report failure Continue to siding Clear switch point	If speed > 8 mph then MISHAP Else continue to siding & clear switch point	Stop train Continue to siding Clear switch point	If speed > 8 mph then MISHAP Else continue to siding & clear switch point	If speed > 8 mph then MISHAP Else continue to siding & clear switch point
$P_F(t)$ - Null	Stop train Report failure Await repair Continue to siding Clear switch point	MISHAP	MISHAP	MISHAP	MISHAP

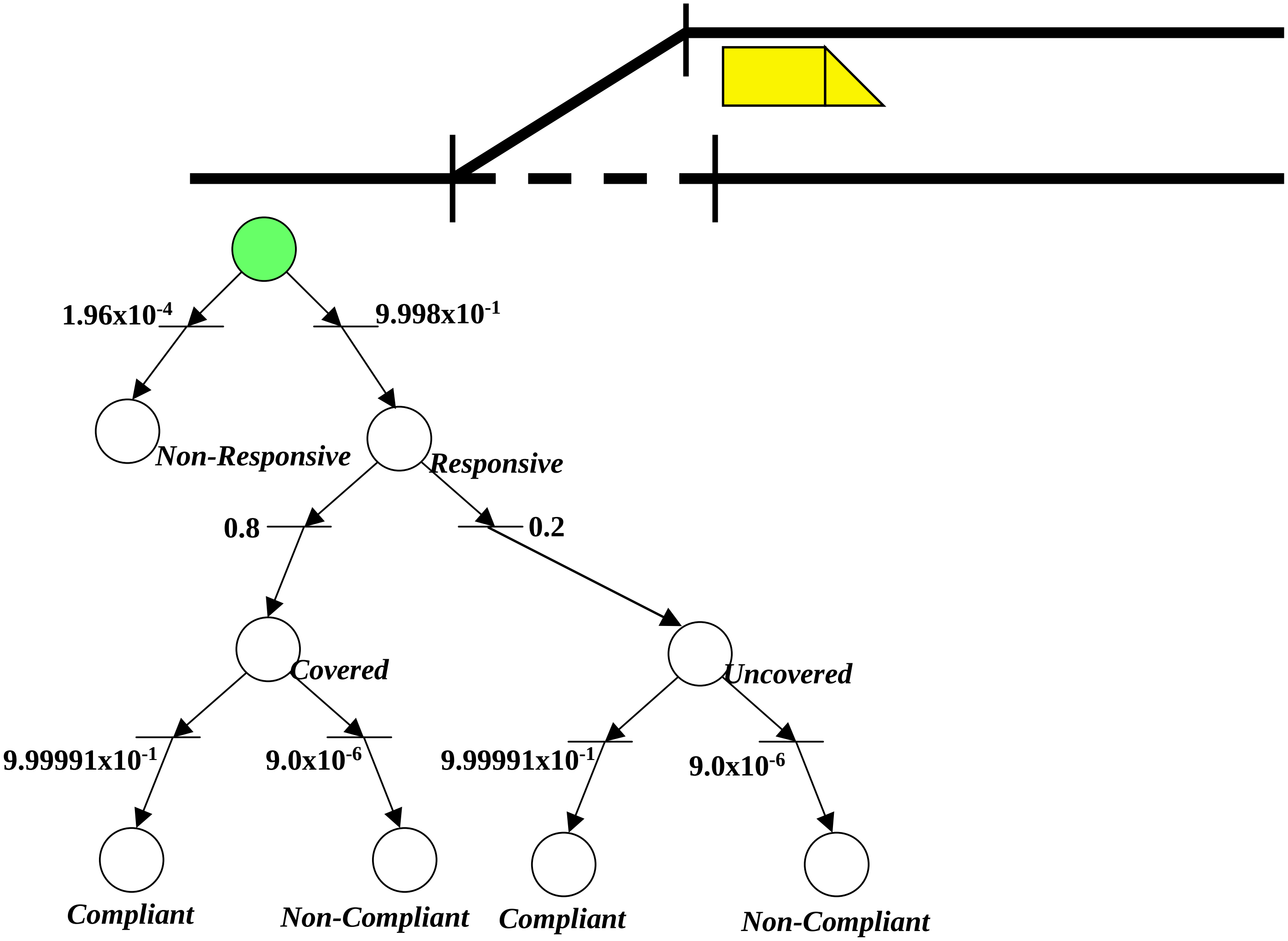
ASCAP IN ACTION



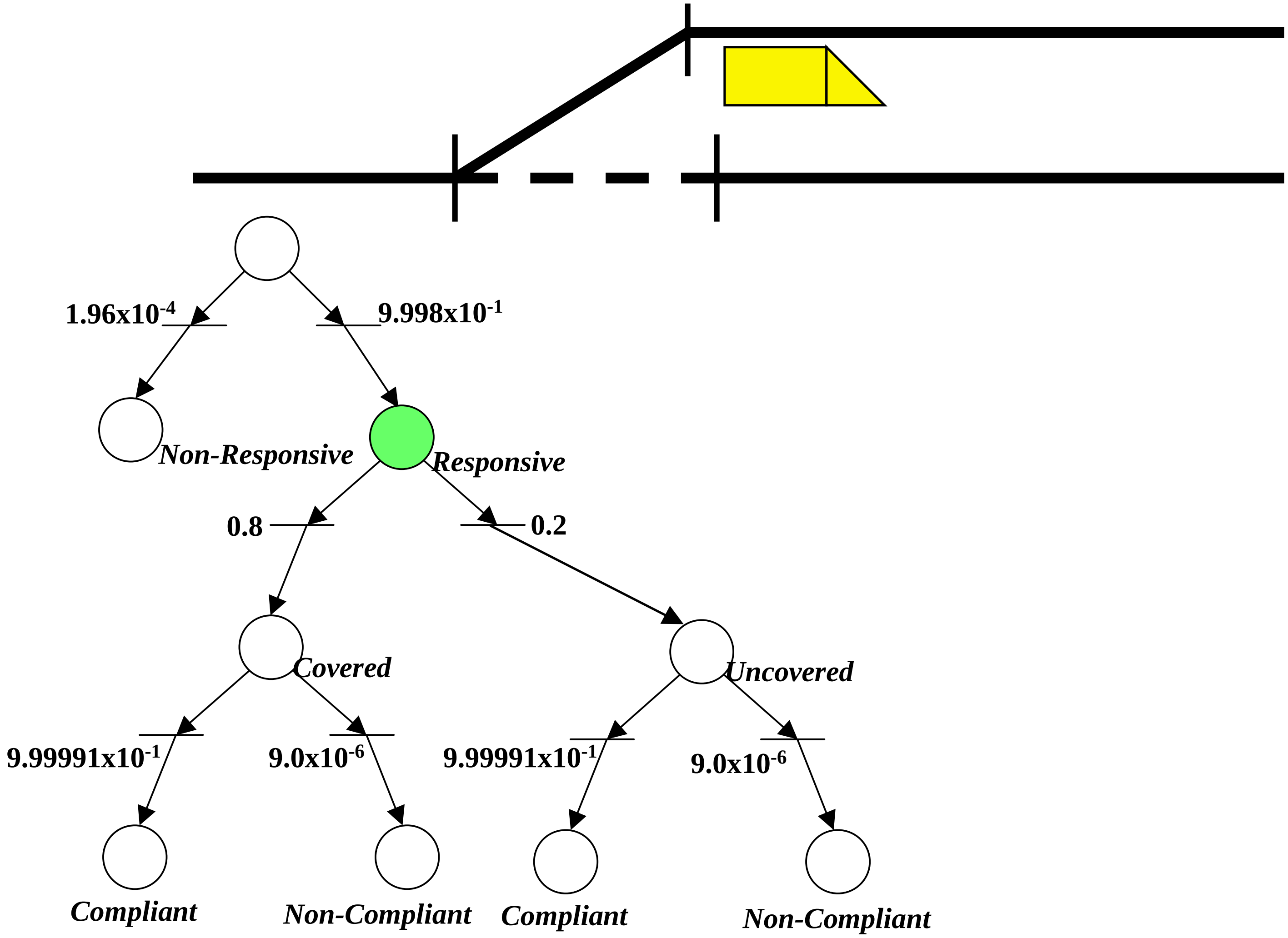
ASCAP IN ACTION



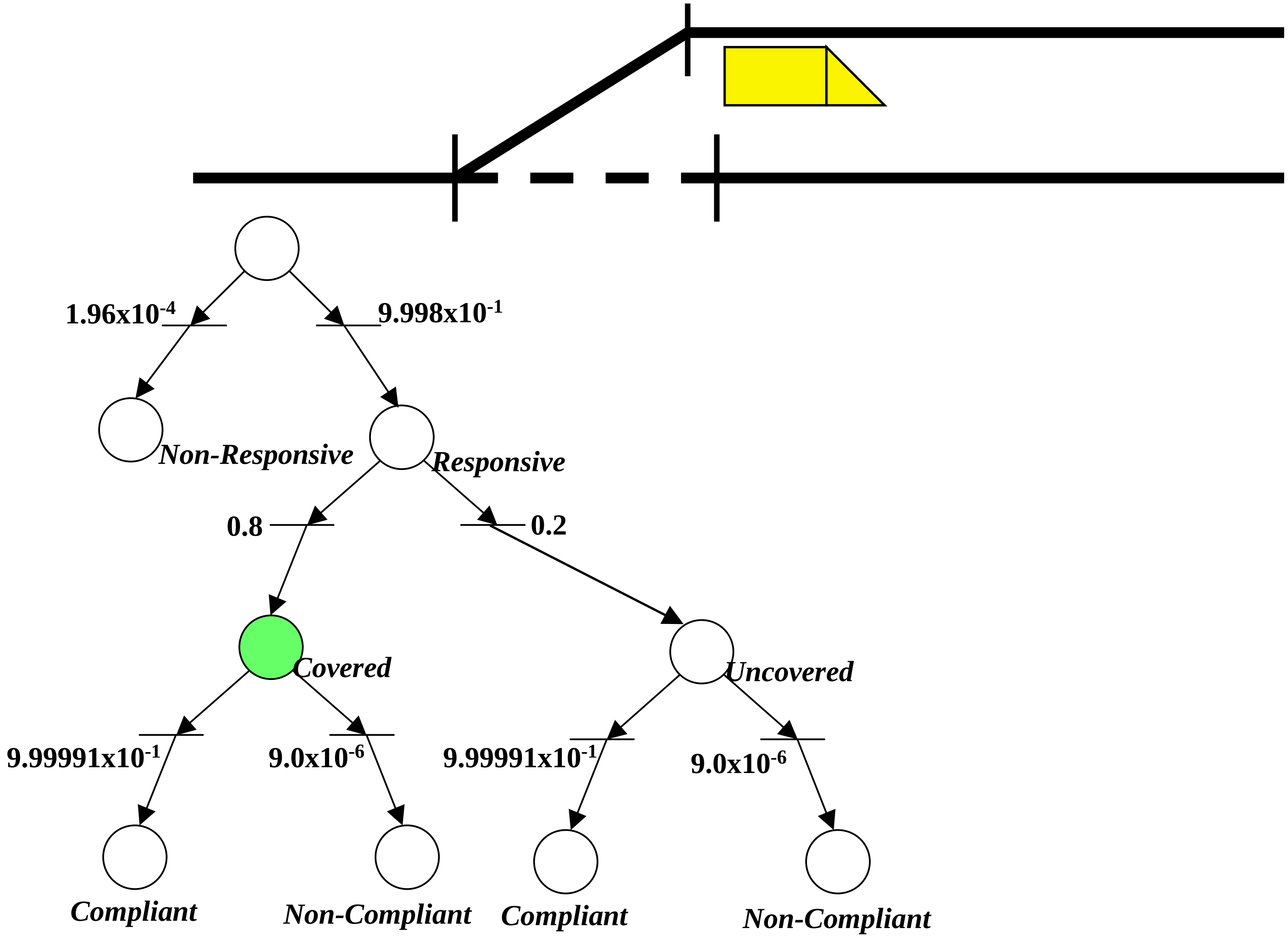
ASCAP IN ACTION



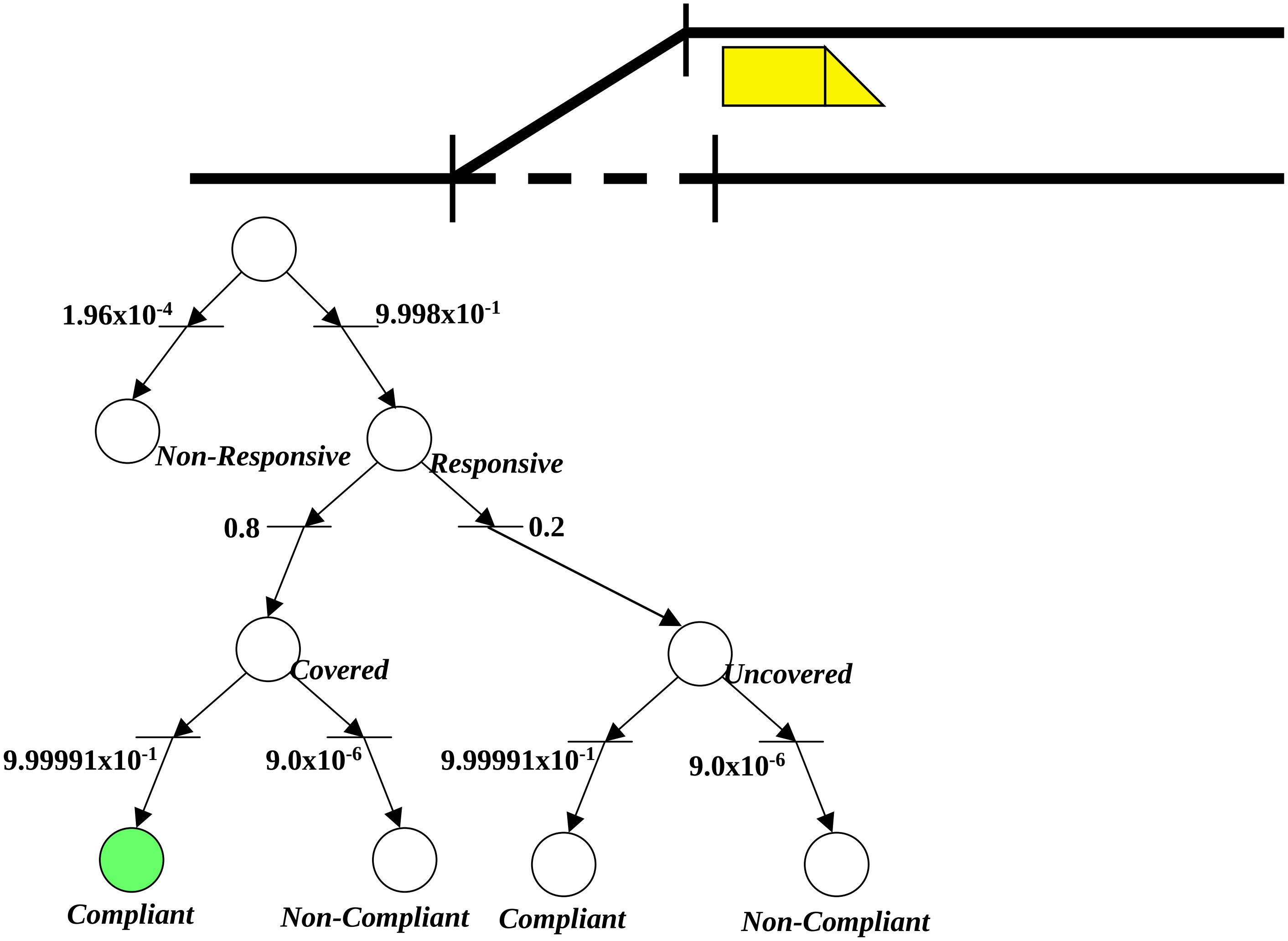
ASCAP IN ACTION



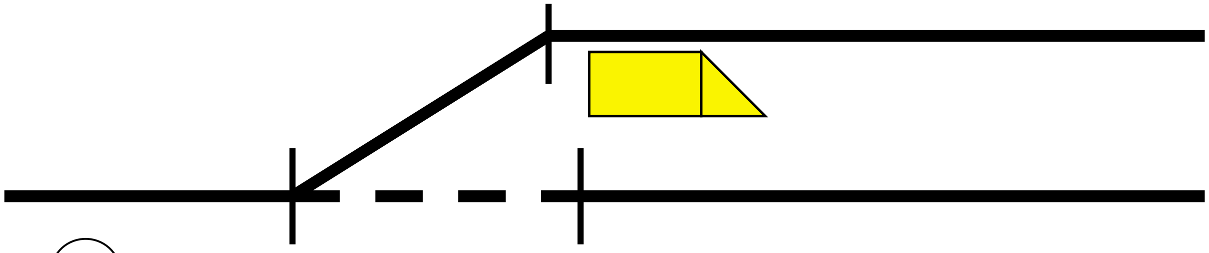
ASCAP IN ACTION

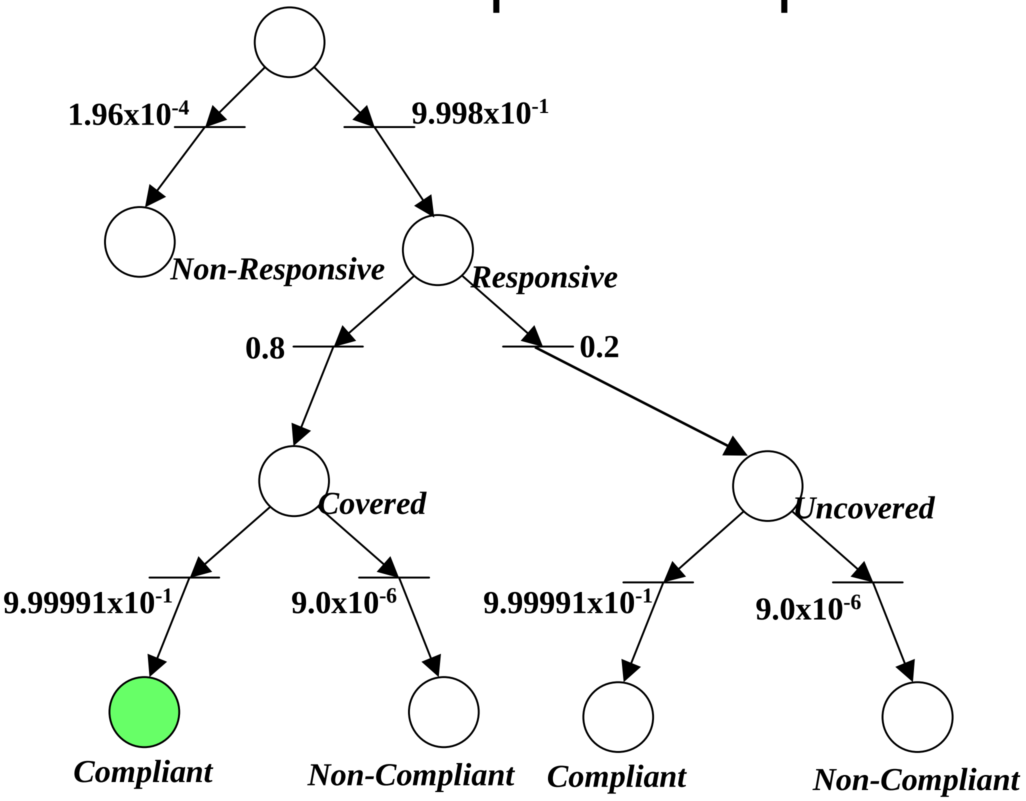


ASCAP IN ACTION



ASCAP IN ACTION





1.96x10^{-4}

9.998x10^{-1}

Non-Responsive

Responsive

0.8

0.2

Covered

Uncovered

9.99991x10^{-1}

9.0x10^{-6}

9.99991x10^{-1}

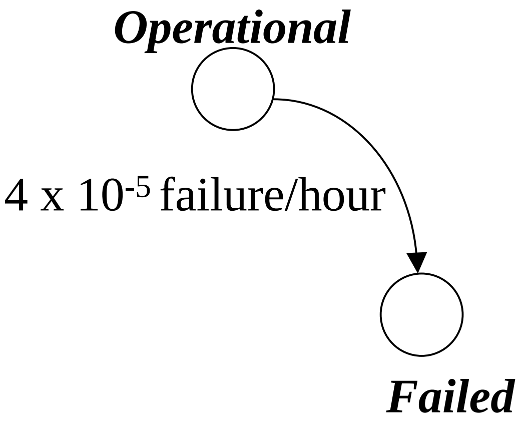
9.0x10^{-6}

Compliant

Non-Compliant

Compliant

Non-Compliant

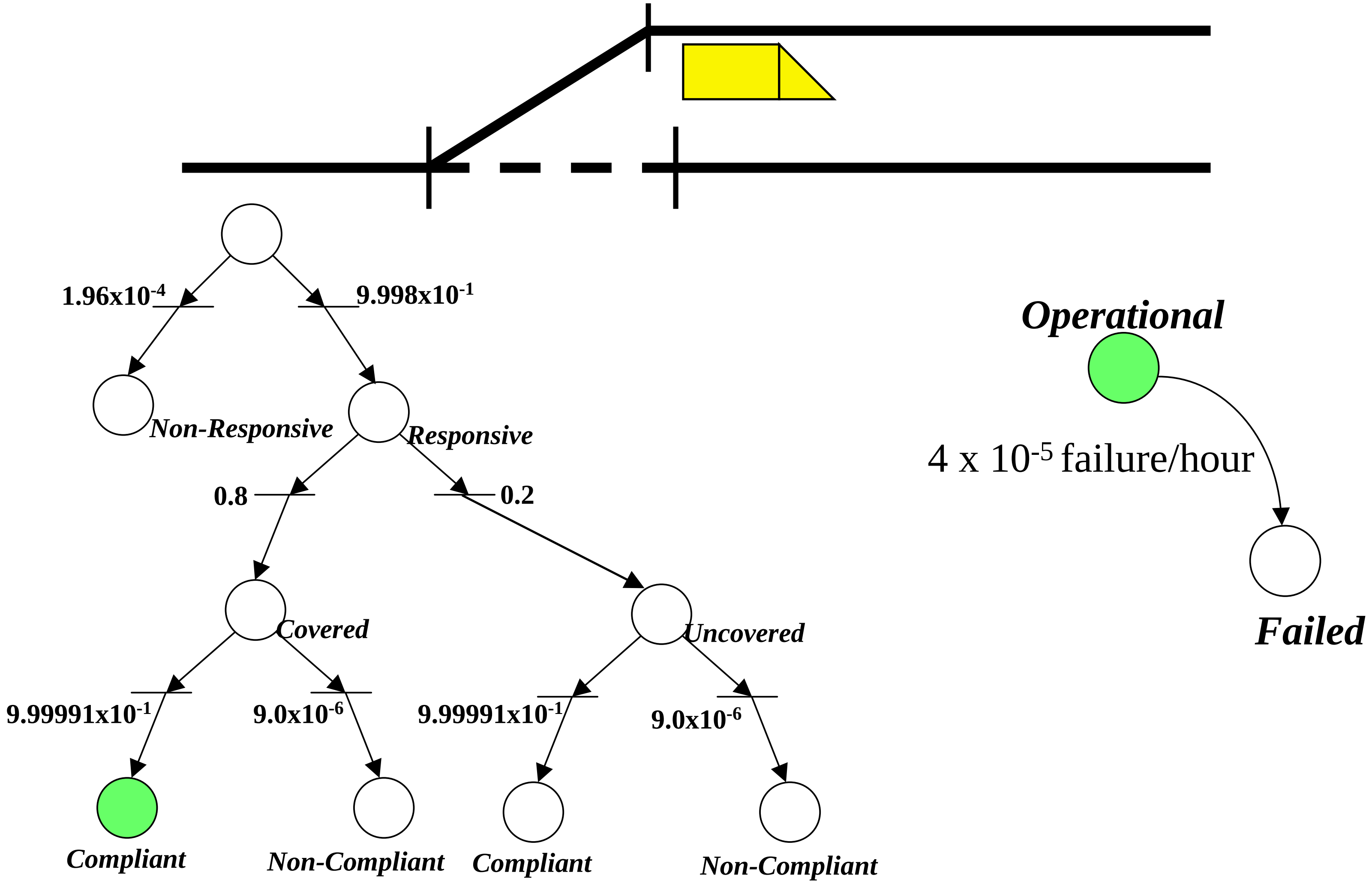


Operational

4 x 10^{-5} failure/hour

Failed

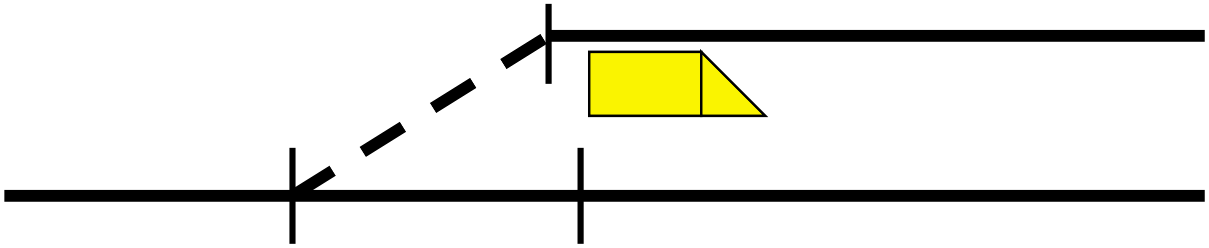
ASCAP IN ACTION



ASCAP IN ACTION

OBJECT STATE	TRAIN CREW BEHAVIOR				
	$P_{CovComp}$	$P_{CovN\text{-}C}$	$P_{UncovComp}$	$P_{UncovN\text{-}C}$	$P_{N\text{-}R}$
$P_O(t)$ - Reverse	Stop train Set normal Continue movement	Continue movement Leave switch reverse	Stop train Set normal Continue movement	Continue movement Leave switch reverse	Continue movement Leave switch reverse
$P_F(t)$ – Reverse, Normal or Null	Stop train after switch Notify for repair /realignment Continue movement	Continue movement Leave switch in failed state	Stop train after switch Leave switch in failed state Continue movement	Continue movement Leave switch in failed state	Continue movement Leave switch in failed state

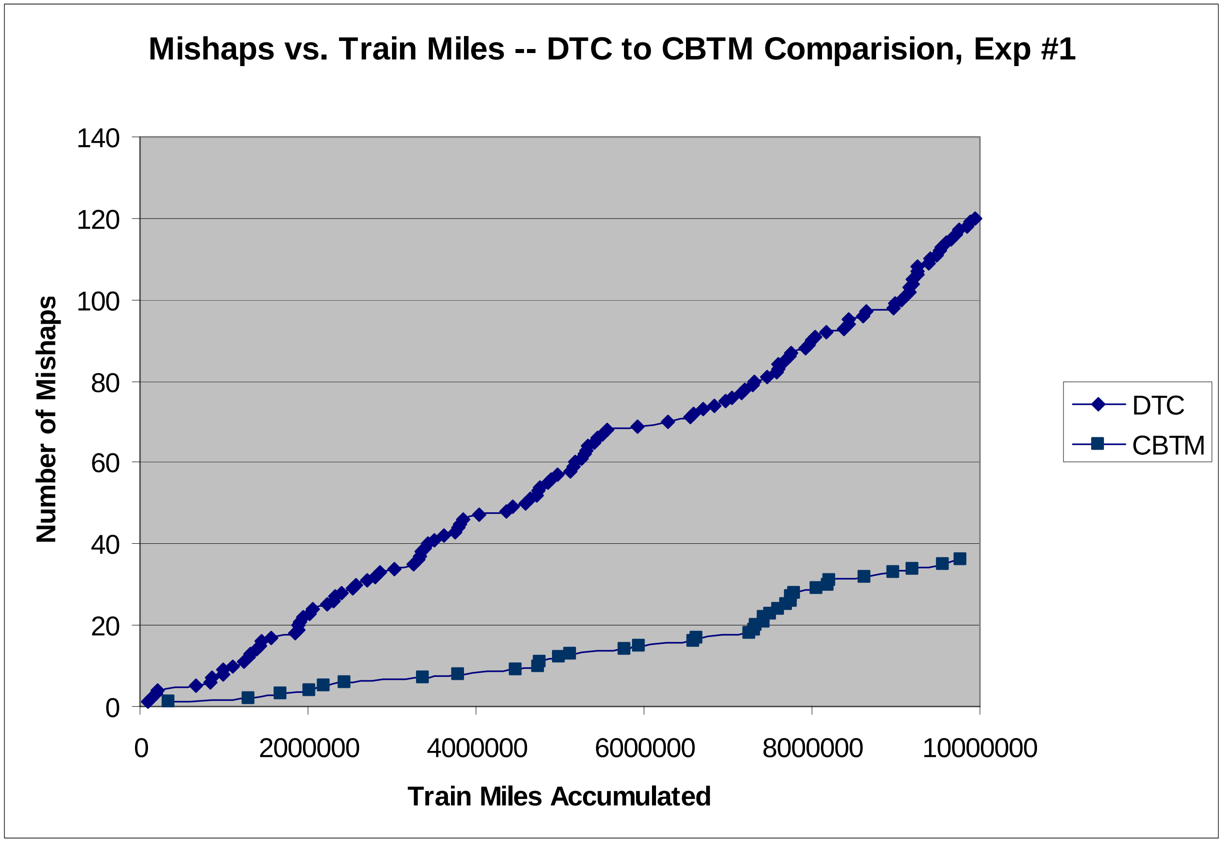
ASCAP IN ACTION



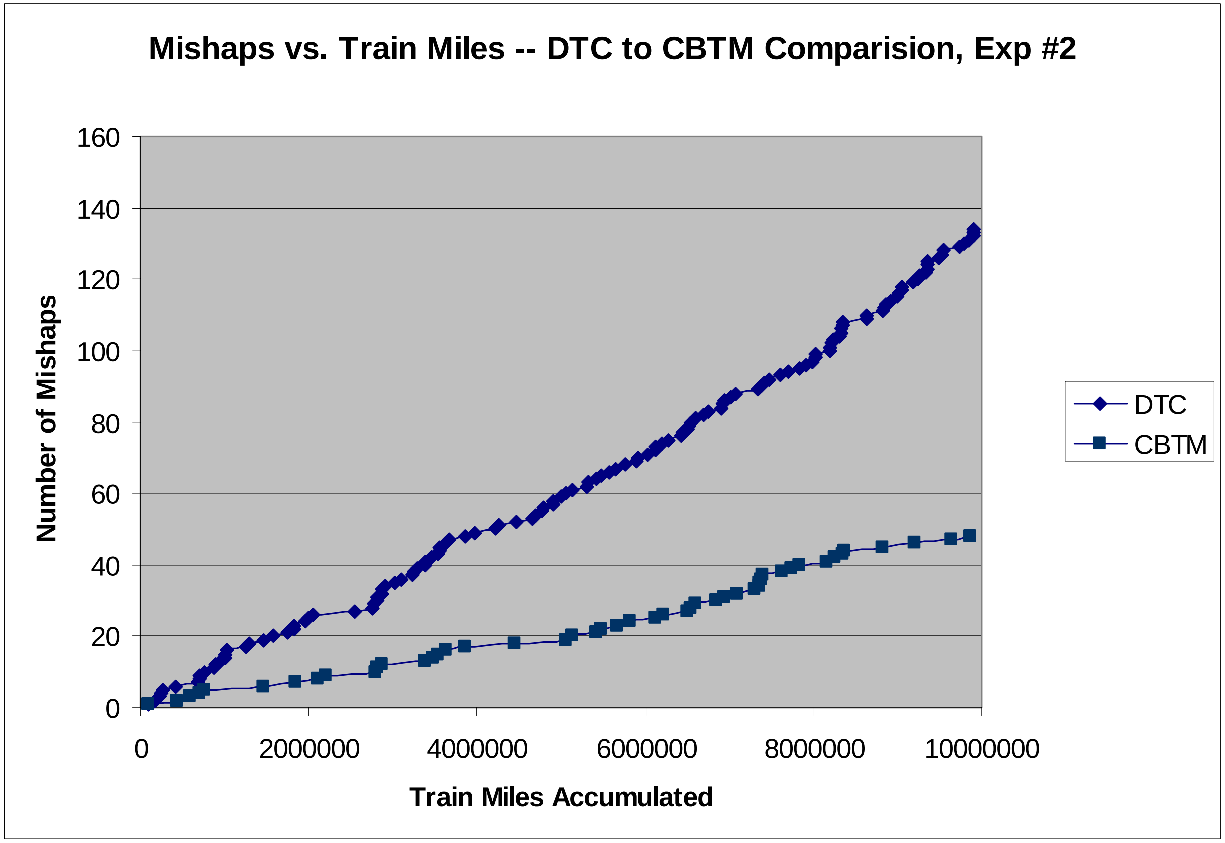
CBTM VERSUS DTC MISHAP RESULTS

- Performed three independent experiments
  - Each experiment lasted for 10,000,000 train miles (~10 years)
  - Each experiment repeated simulation conditions
    - DTC and CBTM simulations occurred in identical environment
    - Allows for statistical comparison of results

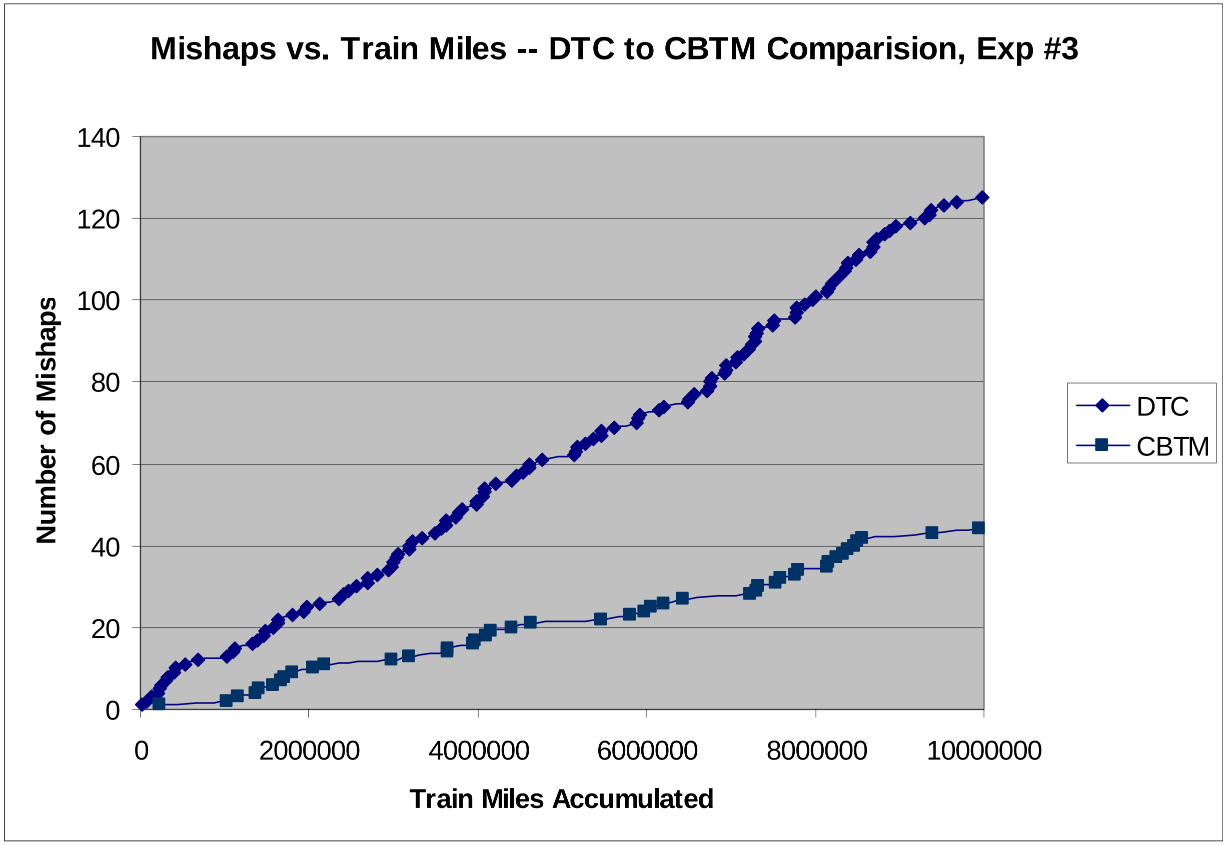
CBTM VERSUS DTC MISHAP RESULTS



CBTM VERSUS DTC MISHAP RESULTS



CBTM VERSUS DTC MISHAP RESULTS


Mishaps vs. Train Miles -- DTC to CBTM Comparision, Exp #3
Number of Mishaps
Train Miles Accumulated
DTC
CBTM